ISAE 3402 and SSAE 16 Accounting Standards

(Type II, SOC 1 assessment)

Reinforcing confidence through demonstration of effective information security and control of service delivery

- **ISAE:** International Standard on Assurance Engagements
- **SSAE:** Statement on Standards for Attestation Engagements

The Growing Trend: Outsourcing companies increasingly depend on third-party providers to deliver critical services. Companies that just a decade ago may have used only one or two third-party services providers now depend on many to deliver a large number of services:

- Application development, testing and maintenance
- Business Process Services
- Cloud computing
- Consulting
- Customer Relationship Management
- Digital Security & Privacy
- IT Infrastructure Services
- Portals & Content Management
- Quality Engineering & Assurance
- Supply Chain Management

These companies are looking for third-party assurance to ratify their internal controls. Accordingly replacing SAS 70 with ISAE 3402 and SSAE-16 standards remains the popular approach to demonstrate third-party assurance.

ISAE 3402/SSAE 16 reporting: -

- Identifies the organization's most business-critical, process-based relationships
- Pinpoints risk prone internal gaps in delivery processes and general computer controls.
- Enhances existing activities with a more comprehensive framework for internal controls - one that achieves compliance with Sarbanes-Oxley financial reporting control requirements (SSAE requirements).

The Relationship between ISAE 3402 and SSAE 16

The SSAE 16 "**attestation**" standard and the ISAE 3402 "**assurance**" standards essentially share a common framework. They are derived from the standards of the Auditing Standards Board (**ASB**) of the American Institute of Certified Public Accountants (**AICPA**). The ASB put forth SSAE 16, and the International Auditing and Assurance Standards Board (IAASB) of The International Federation of Accountants (IFAC), put forth ISAE 3402.

This common framework on which SSAE 16 and ISAE 3402 is based represents is a migration, adoption, and ultimately an acceptance of more globally accepted accounting standards, such as those of the International Financial Reporting Standards (I**FRS**), which are essentially the standards, interpretations and frameworks adopted by the International Accounting Standards Board (**IASB**).

Benefits of ISAE 3402 and SSAE 16 (dual assessment)

With the recent heightened awareness to operational risk management, more and more clients of service organizations are requesting a service organization control (**SOC**) report to provide comfort over existing processes. This dual assessment report is very relevant for the USA as well as Europe and is becoming popular in other parts of the world as well. This covers operational and information security controls in the delivery processes. The key benefits are:

- Strengthening the organization's credentials
- Assisting in fulfilling audit responsibilities of customers and their independent auditors
- Demonstrating that controls are designed and implemented based on an accepted internal control framework
- Providing examinations under an internationally recognized standard as well as under one specific to USA but independent of any control environment.

Overview of Service Organization Control (SOC) reports – SOC 1, SOC 2 & SOC 3

Control reports of service organizations are reports on the internal control structure that relate to transaction processing services. The objective of a control report is to provide clients of the service organization and their independent auditors with information on policies, procedures and controls that may be relevant to their internal control structure and their functional statements. The clients use the report to understand the adequacy and operating effectiveness of their services provider's controls. There are three different SOC reporting options and organizations are to choose one that is the appropriate the organization.

	SOC1	SOC2/SOC3
Focus	Internal control over financial reporting	Operational controls
Scope	• Focused on financial reporting risks and controls specified by the service provider. • Procedures for processing and reporting transactions • Handling of significant events and conditions other than transactions • Other aspects relevant to processing and reporting user transactions	• Infrastructure • Software • Procedures • People • Data
Domains Covered	• Service delivery related controls • Supporting general Information Security controls	• Security • Availability • Confidentiality • Processing Integrity and/or • Privacy

Level of Standardization	• Control objectives are defined by the service provider and may vary depending on the type of service provided	• Principles are selected by the service provider. • Specific pre-defined criteria are used rather than control objectives.

Assessment of our internal control maturity:

Contingent to the maturity of a service organization viz-a-viz the internal control framework, it could choose any of the two types of ISAE 3402/SSAE-16 reports:

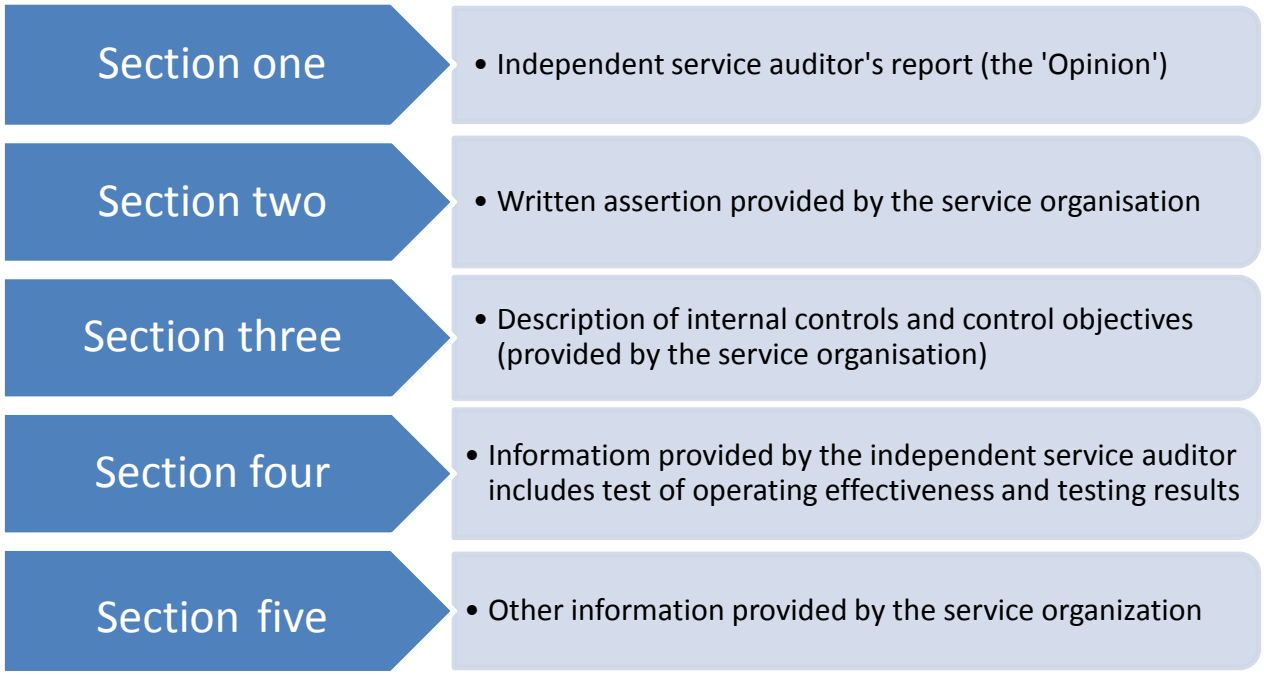
Type 1 report covers controls placed on operations as of a point in time and is considered to be of limited use. It does not cover the operating effectiveness of the controls. Typically, service organizations undertake a Type I examination only in their first year of going through such an examination as they perhaps lack documentary evidence supporting the operating effectiveness of the controls.

Type II report covers controls placed on operations and tests of operating effectiveness for a period of time (generally between 6 months and 12 months). This type of report may be utilized by clients and their auditors for audit control purposes. The differentiating factor is that a Type II report includes test of operating effectiveness and the corresponding results.

Case Study: SQS India BFSI and the assessment firm jointly selected the Type II report based on their confidence in implementation effectiveness.

Type I – ISAE 3402 or SSAE 16 report (Reports on controls placed on operations)	**Type II ISAE 3402 or SSAE 16 report** (Reports on controls placed on operations and tests of operating effectiveness)
• Report controls placed on operations (as of a point of time) • Looks at the existence and design of controls – and not at their operating effectiveness • Considered for information purposes only • Not considered useful for purposes of reliance by auditors • Generally performed in the first year a service organization has acquired a ISAE 3402/SSAE 16 certification	• A report on controls placed on operations and tests of operating effectiveness (for a period of time, between 6 months and 12 months • Differentiating factor, includes tests of operating effectiveness • More emphasis on evidential matter • Requires more internal and external effort • May provide the user auditor with a basis for reducing audit procedures at the service organization

ISAE 3402/SSAE 16 report structure:



The independent assessment report as per ISAE 3402/ SSAE 16 standards provide the confidence in control procedures, adequacy and reasonable assurance in service delivery and information security related controls. It illustrates the positive effects of a properly functioning and articulated control environment to an organization's senior management and our clients.